NASA/TM-2009-215406

Analysis of Space Shuttle Ground Support System Fault Detection, Isolation, and Recovery Processes and Resources

Anthony R. Gross
NASA Ames Research Center

Michael Gerald-Yamasaki
NASA Ames Research Center

Robert P. Trent
NASA Ames Research Center

December 2009

NASA/TM-2009-215406

Analysis of Space Shuttle Ground Support System Fault Detection, Isolation, and Recovery Processes and Resources

Anthony R. Gross
NASA Ames Research Center

Michael Gerald-Yamasaki
NASA Ames Research Center

Robert P. Trent
NASA Ames Research Center

National Aeronautics and
Space Administration

Ames Research Center
Moffett Field, California

December 2009

Acknowledgments

The authors gratefully acknowledge the assistance of A.H. Vera and his staff for access to the Problem Reporting and Corrective Action (PRACA) database.

Available from:

NASA Center for Aerospace Information
7115 Standard Drive
Hanover, MD 21076-1320
443-757-5802

National Technical Information Service
5285 Port Royal Road
Springfield. VA 22161
703-487-4650

Table of Contents

.

Analysis of Space Shuttle Ground Support System Fault Detection, Isolation, and Recovery Processes and Resources

A. R. Gross[1], M. G. Yamasaki[2], and R. P. Trent[3]

Ames Research Center

SUMMARY

As part of the FDIR (Fault Detection, Isolation, and Recovery) Project for the Constellation Program, a task was designed within the context of the Constellation Program FDIR project called the Legacy Benchmarking Task to document as accurately as possible the FDIR processes and resources that were used by the Space Shuttle ground support equipment (GSE) during the Shuttle flight program. These results served as a comparison with results obtained from the new FDIR capability. The task team assessed Shuttle and EELV (Evolved Expendable Launch Vehicle) historical data for GSE-related launch delays to identify expected benefits and impact. This analysis included a study of complex fault isolation situations that required a lengthy troubleshooting process. Specifically, four elements of that system were considered: LH2 (liquid hydrogen), LO2 (liquid oxygen), hydraulic test, and ground special power.

[1] AST, Technical Management, NASA Ames Research Center, CA 94035

[2] Computer Engineer, NASA Ames Research Center, CA 94035

[3] Information Technology Specialist, NASA Ames Research Center, CA 94035

I. Introduction and Objectives

Integrated Systems Health Management (ISHM) is a system engineering discipline that addresses the design, development, operation, and life cycle management of components, subsystems, vehicles, and other operational systems. The primary objectives of ISHM are to maintain nominal system behavior and function, and to assure mission safety and effectiveness under off-nominal conditions.

As an approach to developing a new Fault Detection, Isolation, and Recovery (FDIR) capability for the CxP (Constellation Program), the FDIR Project was chartered to build and implement an FDIR capability for the new ground support equipment (GSE) system being developed for the Aries launch vehicle.

The principal objective of the Fault Detection, Isolation, and Recovery (FDIR) project is to mature the technology, define the architecture and the concepts of operation such that ISHM tools are developed that will provide fault detection, isolation, and recovery for CxP ground operations. This in turn will help meet launch availability rate through faster fault isolation and recovery recommendation; develop the architecture for integrated fault detection, isolation, and recovery (both ground and vehicle); as well as identifying paths for certification of the FDIR architecture and assessments of the FDIR capability, scalability, performance, costs, and benefits.

As part of the FDIR (Fault Detection, Isolation, and Recovery) Project for the Constellation Program, a task was designed within the context of the Constellation Program FDIR project called the Legacy Benchmarking Task to document as accurately as possible the FDIR processes and resources that were used by the Space Shuttle ground support equipment (GSE) during the Shuttle flight program. These results served as a comparison with results obtained from the new FDIR capability. The task team assessed Shuttle and EELV (Evolved Expendable Launch Vehicle) historical data for GSE-related launch delays to identify expected benefits and impact. This analysis included a study of complex fault isolation situations that required a lengthy troubleshooting process. Specifically, four elements of that system were considered: LH2 (liquid hydrogen), LO2 (liquid oxygen), hydraulic test, and ground special power.

Legacy Benchmarking Task Members

Anthony R. Gross	ARC	Exploration Technology Directorate
Michael Gerald-Yamasaki	ARC	NASA Advanced Supercomputing Division
Robert P. Trent	ARC	Intelligent Systems Division

II. Approach

Two basic approaches were taken to obtain the data necessary to meet the objectives of this task:

1. Review and assess pertinent Shuttle-based documents:
   a. System Assurance Analysis (SAA)
   b. Critical Items List (CIL)
   c. Problem Reporting and Corrective Action (PRACA) database, and

2. A field trip to KSC (Kennedy Space Center) to meet with Shuttle GSE operators, including a tour of the related physical systems.

These two approaches will be described in the following sections.

1. a. System Assurance Analysis (SAA)

Liquid Hydrogen System
System Assurance Analysis of the Main Propulsion System Liquid Hydrogen Ground Control System at Pad-A, B, MLP-1, 2, 3, and VAB
SAA09PP03-001, Rev. H, October 2007
File name: SAA09PP03-001_RevH_SAA_MPS_LH2_Part1.ppdf [1082 pages]
File name: SAA09PP03-001_RevH_SAA_MPS_LH2_Part2.pdf [1077 pages]

Liquid Oxygen System
System Assurance Analysis of the Main Propulsion Liquid Oxygen Control System for the Launch Operations Area (Pad A/B) and the Vehicle Assembly Area
SAA09PP02-001, Rev. H, March 1990
File name: SAA09PP02-001_RevH_SAA_MPS_LOX.pdf [301 pages]

Hydraulics Support System
System Assurance Analysis of the Orbiter / Solid Rocket Booster Hydraulic Support System
SAA09HS01-001, Rev. D, July 2006
File name: SAA09HS01-001_RevD_SAA_Orbiter-SRB_Hydraulics.pdf [212 pages]

Ground Special Power System
System Assurance Analysis of the Special Power System at the Kennedy Space Center
SAA00037, Rev. A, January 2008
File name: SAA00037_RevA_SAA_Special_Power_at_KSC.pdf [2013 pages]

1. b. Critical Items List (CIL)

Derived from the FMEA (Failure Modes and Effects Analysis), the CIL documents failure modes that are deemed "critical" by program definition. FMEA/CIL Criticality is used throughout the Program for determining the appropriate level of visibility and risk management. For details of the Critical Items List, see Appendix A below.

1. c. Problem Reporting and Corrective Action (PRACA) Database

PRACA, as applied to the Space Shuttle Program, is designed to be both a process and a database. The PRACA process attempts to provide consistent processing and resolution techniques; supports effective technical investigation, analysis, and closure of reported problems; and supports evaluation of test programs for effectiveness. These processes also assure that problems will receive adequate visibility and review at appropriate levels of management to support effective risk management and mission success.

2. Field Visit to KSC

A two-and-a-half-day trip to KSC was undertaken to meet with the domain experts and system operators of the four selected GSE systems, as well as to observe the associated hardware systems. This was necessary to provide 'ground truth' to the assessments made from the PRACA database and the other reference documents that were made available to this task.

The team met with the following KSC GSE operations personnel:

LH2/LO2 Systems	Diane Stees Mark Berg Miles Ashley
Hydraulics Support System	Kip Anderson Carla Rekucki Slade Peters
Ground Special Power System	Douglas Bearden

For each GSE system the processes that were used to identify, isolate, and repair major problems, as well as approximate actual timings were reviewed and discussed. The relevance and utilization of the PRACA database records identified by the Ames task team were also reviewed and discussed.

In addition, two tours of the GSE hardware systems were provided in the vehicle assembly building (VAB) and on the mobile launch platform (MLP), one for the Hydraulics Test System, and one for the Ground Special Power System. Each tour provided the opportunity for the Ames task team to gain a more in-depth understanding of the system components and interactions, as well as to understand the actual fault detection, isolation, and repair processes used by the system operators.

As a result of the analytical work done at Ames, as well as the discussions and tours at KSC, the following observations, examples, conclusions, and recommendations were developed:

Observations and Processes Common to All Systems

Given that the objectives of the Legacy Benchmarking task were to identify the processes and resources utilized in the FDIR processes for the Space Shuttle Program, the following results for all four GSE systems became clear:

1. The PRACA database was of limited value in meeting the objectives of this task. While it did provide a good, if sometimes confusing, introduction to the four GSE systems, its overall lack of comprehensiveness and consistency in data entry made it particularly difficult to draw any significant conclusions. This observation was corroborated by all of the KSC operators with whom we discussed this topic. There were, however, a few example entries that will be cited in this report that did provide useful information to this task.
2. Domain expertise and long experience possessed by many of the system operators facilitated a very rapid response to, and identification of, system anomalies and failures.
3. Careful and extensive maintenance procedures, developed over the entire Space Shuttle Program, have served to minimize system anomalies in many of the systems. The Ground Special Power System is a particular example of a system with an extensive maintenance program, in which Doug Bearden reported that more than 90% of identified anomalies were found during the maintenance process.
4. Most of the GSE operators had only a rudimentary knowledge of the three FDIR computer tools that are being developed as part of the FDIR Project.

Observations, Processes and Examples - LH2/LO2 Systems

The information used for this section of the report includes:

- System Assurance Analysis (SAA) of the Main Propulsion System Liquid Hydrogen Ground Control System (September 2007)
- System Assurance Analysis (SAA) of the Main Propulsion Liquid Oxygen Control System (March 1990)
- PRACA database
- Report on Launch Countdown History
- Space Shuttle Operations and Infrastructure – A Systems Analysis of Design Root Causes and Effects, Carey M. McCleskey
- Interviews with LH2/LO2 system engineers

The Critical Items List (CIL) in the SAAs for Liquid Hydrogen (LH2) and Liquid Oxygen (LO2) contains a description of critical items, their failure modes, and detection methods. The SAA for LH2 lists 196 items and the LO2 SAA lists 15 items in the CIL (A revised SAA is in preparation lists 124 CIL items). Most of these items describe a detection method of a visual on console and few assign a correcting action to mitigate the critical failure effect.

The SAA for LH2 was updated in September 2007 and includes in the CIL the results of a search through the PRACA database for test failures, unexplained anomalies, and other failures experienced during ground processing activities for each item in the CIL. The great majority of these faults were detected through routine operations, test, and/or maintenance with routine recovery from the fault. Few of the PRACA records reported failures of the CIL item in the critical failure mode. There were no catastrophic failures.

Additional searches and analysis of PRACA records yield similar results: a vast majority of the problems reported is handled in a routine manner, that is, faults are detected in the normal course of operations, and isolation and recovery are routine.

Engineers for these systems describe problems that are either:

- Really simple – a gauge or transducer fails; quick detection from a visual observation on the console; and known recovery strategies due to familiarity with problem are employed. Very short times for detection, isolation, and recovery, a scale of minutes.

- Really complicated – unfamiliar – not seen before, not thought about before and lack of understanding of problem, data gathering, data analysis and trouble-shooting make for a lengthy process to isolate and recover from these faults, a scale of days or weeks.

- Very few problems fall in between with a scale of hours

The complicated problems are described as stemming from:

- Faults from unanticipated errors or conditions

- Faults propagated from other systems or subsystems (outside the scope of monitoring for the LH2/LO2 systems)

The process used for detecting problems, isolation, and recovery follows a fairly predictable course:

1. A measurement anomaly, system indicator on the console, or an announcement over the net of a problem (an example given by the engineers was an announcement over the net of an imminent loss of vehicle power)

2. Diagnose problem from available information or gather more information about the problem (e.g., send a technician out to gather information at the site)

3. Recovery procedures are employed

The time to diagnose a problem is highly dependent on the quality of immediately available salient information. Once a diagnostic process enters into a phase of seeking additional information, the time to recovery increases dramatically (i.e. goes from "really simple" to "really complicated"). Even a need for less complex information gathering, such as a technician verifying equipment conditions at the site, requires lengthy procedural costs in terms of time to recovery.

Three example cases for LO2 are presented below. This information was provided by the systems engineer Miles Ashley from problem documentation, console logs, and personal memory. The PRACA database, while presenting a comprehensive record of problems, is less effective as a source for understanding the processes involved in diagnosing problems and the length of time required from detection to recovery. A power loss problem immediately subsequent to the STS-116 liftoff was discussed by the systems engineers as a notably challenging problem. The PR for this incident as presented in PRACA is summarized following the three example cases. Note the understated presentation of this report. No hardware criticality was assigned to this PR.

Example Cases

1. Easy Troubleshooting Complexity

IPR PadA-2538 / PR S72-0813-00-001-1104
This PR happened during OMI G2115 LO2 pump test. The A86538 pump common suction line temperature transducer FD GLOT0207A was reading off-scale-high (-274 deg f) during the entire test in which LO2 temperatures (-295 deg f) should have been experienced by the transducer.
Problem Type: Instrumentation failure
Indications: Off-scale high measurement

Troubleshooting steps:

1. Other measurements on same fuse/chassis/slot verified for accuracy.
2. Measurement was not bypassed and test continued based on single fault instrumentation failure. Fault classified as" instrumentation" based on flow conditions and validity of other measurements.
3. Post-test troubleshooting (pad electrical engineering) consisted of using a 0-5 volt transducer checkout box. It confirmed a bad transducer.
4. Transducer was replaced

Time of detection: approx 1538GMT 2/9/07
Time to diagnosis: <30 seconds (exact time cannot be determined, but operator detected problem immediately after A4 block valve was opened. Procedure is to open valve and then monitor for temperature <-290F. Time for this temperature shift from ambient is seconds.
Time elapsed to diagnosis of problem: < 30 seconds

2. Medium Troubleshooting Complexity

IPR-PADA-2523 / PR S72-0694-17-002-0203 A106425 Closed Indicator Is On Should Be Off.
During OMI T2405 (Nose Cone Purge Panel System Leak Check) the A106425 ball valve closed indicator (GLOX4193E) was on after the ET nose cone purge redundant shutoff valve disable command (GLOK4190E) was issued. The valve-closed indicator should have been off indicating the valve was open.
Problem Type: Valve indicator not in expected state
Indications: A106425 valve position display indicated closed (expected state was open)

Troubleshooting steps:

1. Testing continued around fault
2. Console engineer researched command pathway using electrical schematics
3. Real time continuity check between valve indicator pins accomplished by technician in field (continuity was good).
4. IPR troubleshooting plan developed (1/31/07)
5. System powered-up to record state of valve indication
6. Voltage measurements taken in remote distributor
7. Visually verified actual position of valve
8. System powered down, demated cables, shorted cable pins together, power up and obtained resistance readings to check for shorts.
9. Verified valve position
10. System powered down
11. Cross connect redundant shutoff valve cable, powered up and verified valve position
12. Troubleshooting indicated the pneumatic valve was showing open and closed at the same time due to an internal fault in the position indicator. Command pathway was OK.
13. Valve was replaced.

Time of detection: 1429 GMT 1/29/07
Time to diagnosis: 1448 1/31/07
Time elapsed to diagnosis of problem: 2 days

3. Hard Troubleshooting Complexity

IPR PADA-2603 Helium Bubbling Delta Pressure Anomaly
During STS-117 launch countdown, both the primary and secondary helium bubbling delta pressure transducers began indicating positive pressure at T-1M44S. This was after helium bubbling was terminated. The measurements should have been zero (or near their bias for zero flow). Other indications of helium bubbling termination (GHe bubbling supply pressure and primary/secondary control solenoid valve positions)

were reading nominally at the time. Even though the flow indication on the secondary transducer was greater than the LCC limit (ET-03), the countdown was continued because this was considered a voting logic anomaly outside the LCC affectivity. Post-launch troubleshooting revealed no discrepancies with GSE helium bubbling hardware. Extensive post launch data analysis for STS-117 and previous missions indicate that these transducers are very susceptible to upstream pressure fluctuations. This pressure transducer activity has been seen at both pads on previous missions under similar conditions (countdown time, GHe demand, etc). The differential pressure transducers were also shown to indicate positive flow under reversed flow conditions. The STS-117 anomaly occurred coincident with a high GHe demand from the hydrogen vent flex line purge and subsided when this demand ended. Based on the data, the anomalous behavior was caused by pressure disturbances in the helium supply during periods of high demand and is an explained condition. The condition is expected to recur under similar circumstances. Per Launch Director/ Test Team agreement, no notification of a similar occurrence during launch countdown will be made. Hardware modifications are under consideration to mitigate transducer sensitivity. Probable cause: Explained Condition

Problem Type: Unexpected flow measurement (limit exceeded)
Indications: both primary and secondary helium bubbling delta pressure measurements began indicating positive pressure. Secondary measurement indicated a maximum of 0.152 psid, which exceeds the LCC ET-03 limit of 0.1 psid. Primary measurement indicated a maximum of 0.096 psid. Delta press measurement range is 0–2 psid

Troubleshooting steps:

1. A No Hold LCC call was made at T-45S as required by LCC IMPL-01 section 1.2.B LCC Outside of Time Period Effectivity. Countdown was continued.
2. Extensive data review was conducted post launch (included previous five missions)
3. Helium bubbling system passed leak check from panel supply valve to GUCP connection flex hose with bubble soap and 45-minute pressure decay check (6/12/2007)
4. Attempted to recreate delta pressure excitation by cycling LH2 purges ON/OFF in Terminal Count sequencing. No indications seen on helium bubbling delta pressure measurements (6/15/2007)
5. S72-0697-08 panel joints torqued per OMI T2408. Slight movement seen on A78427 panel outlet bulkhead fitting to tubing B-nut connection (6/18/2007)
6. S72-0697-08 panel leak and functional validation per OMI T2404.001 complete with no anomalies (6/25/2007)
7. Internal seat leak check performed across A78411/412/413 valves. No leaks noted (6/27/2007)

8. low reversed through venturi by venting system through A86903 vent valve. Delta press measurements indicated flow. Supply pressure made erratic by rapidly cycling A86903 vent valve open/close. Delta press measurements indicated flow (7/6/2007)

Time of detection: 233620 GMT 6/8/07
Time to diagnosis: 7/7/07
Time elapsed to diagnosis of problem: 29 days

PRACA Report I-V6-442728 (Excerpts)

Project:	UNKNOWN-UNKNOWN
Element:	UNKNOWN
Engineering Group:	ECL
Current EICN:	117V-0054
Work Area:	OPF-1
Detected During:	S0007.200
Problem Description: Disposition:	MULTIPLE PAD B HIMS LOST POWER

[Authors' note: The text that is displayed here is shown exactly as it has been extracted from PRACA. Any errors appear exactly as they occur within PRACA.]

IPR 117V-0054 BEGAN AS IPR 116V-0138 TO DOCUMENT LOSS OF POWER TO PADB/MLP 1 HIMS SHORTLY AFTER LIFTOFF OF STS-116, OV-103. SEVERAL OTHERMANIFESTATIONS OF THE POWER LOSS WERE SEEN BY FIRING ROOM PERSONNELWHILE ATTEMPTING POST LAUNCH SECURING. LOX SYSTEM COMMAND ANOMALIESWERE DOCUMENTED ON IPR PADB-3151. GVA HOOD ANOMALIES WERE DOCUMENTED ON IPR PADB-3152. COMMON DATA BUFFER (CDBFR) DATA READS (PVO VS S FD) DIDNOT AGREE AFTER HIM RESETS WERE DOCUMENTED ON IPR FR4-0383.TROUBLESHOOTING OF THE ORIGINAL ANOMALY ISOLATED THE PROBLEM TO ATRIPPED CIRCUIT BREAKER ON THE PAD B UPS 41/41A OUTPUT DISTRIBUTIONPANEL CB 10. THE CB TRIP WAS CAUSED BY A PHASE-TO-PHASE SHORT WITH IN APAD B TO MLP1 INTERFACE CONNECTOR. THE WIDER LOSS OF HIM DATA ANDCONTROL WAS DUE TO THE PAD B UPS

41/41A MAINTENANCE ISOLATION SWITCHHAVING AN UNINTENDED OVERLOAD PROTECTION WITHIN ITSELF. INDUSTRYSTANDARDS REQUIRE UL APPROVED SWITCHES HAVE THIS FEATURE, HOWEVER THEDESIGN SPECIFICATION WAS FOR NO OVERLOAD PROTECTION. IPR 116V-0138 WASTRANSFERRED TO IPR 117V-0054 TO PROVIDE TRACKING VISIBILITY FOR THECORRECTION OF THE GENERIC PROBLEMS WITH ALL LC-39 MLPS AND PADS IDENTIFIED BY THE TROUBLESHOOTING OF THE ORIGINAL ANOMALY. MULTIPLE MAXIMO WORK ORDERS WERE OPENED TO PERFORM THE REPAIR OF THE ORIGINAL ANOMALY AND TO CORRECT THE OTHER CONTRIBUTING FACTORS WHICH DELAYED THEPOST LAUNCH SECURING. ATTACHMENT G LISTS THE MAXIMO WORK ORDERS THATPERFORMED THE PAD B, PAD A, MLP1, AND MLP2 REPAIRS. ATTACHMENT H ILLUSTRATES THE WORK DONE FOR STS-117 ON PAD A AND MLP2. ALL OTHER WORK IDENTIFIED BY THE TROUBLESHOOTING OF THIS ANOMALY WILL STAND ALONE ONTHE WADS OPENED FOR THOSE SYSTEMS. NO FURTHER WORK WILL BE DONE ON THISIPR. IPR 117V-0054 WILL BE CLOSED AS A DUPLICATE OF MAXIMO WORK ORDER772477. ATTACHMENT 1 IS A COPY OF MAXIMO WORK ORDER 772477. CLOSE THIS IPR AS A DUPLICATE OF MAXIMO WORK ORDER 772477.

Observations, Processes and Examples – Hydraulic Support System

The information used for this section of the report includes:

- System Assurance Analysis (SAA) of the Orbiter/SRB Hydraulic Support System at Pad A, 8, VAB, SLF, SLS, OPF 1, 2, 3, and MLP 1, 2, 3 (updated July 2006)
- PRACA database
- Report on Launch Countdown History
- Space Shuttle Operations and Infrastructure – A Systems Analysis of Design Root Causes and Effects, Carey M. McCleskey
- Interviews with Hydraulic Support System systems engineers and operators

Like the LH2 and LO2 systems, most of the Critical Items List (CIL) in the SAA for the Hydraulics Support System describe a detection method of a visual on console and few assign a correcting action to mitigate the critical failure effect. The SAA for the Hydraulics Support System was updated in July of 2006 and includes in the CIL the results of a search through the PRACA database for test failures, unexplained anomalies, and other failures experienced during ground processing activities for each item in the CIL. The great majority of these faults were detected through routine operations, test, and/or maintenance with routine recovery from the fault. Few of the PRACA records reported failures of the CIL item in the critical failure mode. There were no catastrophic failures. Additional searches and analysis of PRACA records yield similar results: a vast majority of the problems reported is handled in a routine manner, that is, faults are detected in the normal course of operations, and isolation and recovery are routine.

The categorization of the difficulty of problems has been given above in the LO2/LH2 section, as well as the sources of the complicated problems, and apply equally well to the Hydraulics Support System.

One of the difficulties for this task that was identified by the Hydraulics Support System engineers was in the problem identification and description process that is in current use. When a problem is initially discovered, it is reported as an Initial Problem Report (IPR). At this stage, the problem has not been isolated, only detected. At some later point in time, duration and process undocumented, the problem becomes isolated and noted as a problem report (PR). Thus, it becomes difficult to determine the time and resources allocated in transitioning from a reported problem to an isolated and diagnosed problem, ready for remediation.

Two particular Hydraulics Support System-related problems were identified and discussed during our meetings at KSC that are out of the ordinary leak problems associated with this system: vibration from a hydraulic pump during testing, and a strong vibration in the hydraulic system when the brakes were applied to the orbiter.

In the first case, there was evidently a problem with one of the pumps in the Hydraulics Support System. The problem was detected by the flight control team and relayed to the Hydraulics Support System engineers. For some reason this pump anomaly was not detected by the Hydraulics Support System team. This problem was still in the process of being resolved at the time of our meeting at KSC, following several days of investigation. This seems like the class of problem that the IMS tool might well have identified much earlier in the sequence.

In the case of the orbiter brake problem a strong vibration was noted when the brakes were applied to the orbiter during a routine test process. Several days and many avenues of discovery were employed to isolate the problem. To date no definitive cause has been found other than to assume that something in the design of the orbiter brake system is responsible. A workaround was developed that ameliorated the problem so as to allow the testing to proceed.

Observations, Processes and Examples – Ground Special Power System (GSPS)

The Special Power System supplies 28 Volts Direct Current (VDC) and 400 Hertz (Hz), 120 Volts Alternating Current (VAC) power to Ground Support Equipment (GSE) and flight hardware at several locations throughout Kennedy Space Center. These locations include Pad-A, Pad-B, Orbiter Processing Facility (OPF)-1, OPF-2, OPF-3, Mobile Launcher Platform (MLP) -1, MLP-2, MLP-3, Space Shuttle Main Engine Processing Facility (SSMEPF) in OPF-3, and the Hypergolic Maintenance Facility (HMF).

In discussions with Ground Special Power System engineers, it was presented that the system is highly redundant, with several backup systems designed to meet a variety of failures and anomalies. Several of these backup systems were observed during our tour of the GSPS. Long experience of many of the GSPS engineers facilitates the rapid identification of potential and actual problems. In addition, it was indicated that normal maintenance procedures were able to catch and repair the majority of the system anomalies before they became a serious problem. Thus, to a large extent, under current practice, the FDIR process in the GSPS is conducted by the operators themselves during normal operations.

However, STS-116 provided a situation in which the GSPS failed in an unexpected manner, which took several days to identify, isolate, and repair the fault. After liftoff, multiple Pad B/MLP HIMS lost power, UPS 41/41A distribution panel circuit breaker 10 and the maintenance isolation switch (MIS) tripped. The failure was traced to a phase-to-phase short in the 480-volt MLP/Pad B interface plug. Extensive electrical system and material analyses were conducted to resolve this issue. Details of this incident may be found in the presentation by the Pad B Power Outage Team on February 9, 2007 entitled “STS-116 Shuttle Processing In-Flight Anomaly Pad B Post Launch Power Outage”.

III. FDIR Project Tool Recommendations

The FDIR Project is developing three computer-based tools:

1. Inductive Monitoring System (IMS).
   The IMS is a software product from Ames Research Center that learns the normal state of a system from training data, and can subsequently identify abnormal input data from that system by comparing the new inputs with the known normal data.
2. Testability and Engineering Analysis Maintenance System (TEAMS).
   TEAMS is a commercial software product from Qualtech Systems Inc. made up of distinct components that can be used together or severally in different configurations. The TEAMS model captures a system's structure, interconnections, tests, procedures, and failures. The model links these failures to the system's built-in tests, troubleshooting steps, and repair procedures.
3. Spacecraft Health INference Engine (SHINE).
   SHINE is a high-speed expert system and inference engine based upon the experience and requirements that were collected over the years by the Artificial Intelligence Research group at NASA/JPL in developing expert systems for the diagnosis of spacecraft health.

During our meetings with the GSE operators, there were brief discussions of these three FDIR tools and how they might be applicable to the operation and monitoring of the four selected GSE systems. A summary of their first impressions as to the potential utility of these tools, admittedly based on only a preliminary understanding of the tools' capabilities, is shown below:

LO2/LH2 Systems	IMS
Hydraulics Support System	IMS, TEAMS
Ground Special Power System	IMS

Further development of the tools, plus demonstrations in an operational environment, will undoubtedly clarify and strengthen their appreciation of the FDIR tools' potential utility.

IV. Conclusions

The primary considerations for effecting the time from fault detection to recovery are the availability of information and the selection of important information from among the available. The human operators of these processes are particularly capable through the accumulation of knowledge and experience of selecting the important information to be applied to the solution of a particular problem.

To have a positive impact on the time from fault detection to recovery FDIR tools must provide either:

- An increase in the quantity of immediately available information about the system and/or

- Assistance in selecting important information for fault detection, isolation and recovery processes

However, simply increasing the quantity of available information will not necessarily have a positive impact on the timeliness of fault detection, isolation, and recovery, if the selection of important information is made more difficult.

The potential benefit of an FDIR system would include extension of available information with assistance in selection of important information to be utilized. Simply putting a sensor on everything would not necessarily improve the performance of fault remediation. Access to broader cross-system information, for instance, would increase the likelihood of important information reaching the right operator, but at the cost of the need to filter increased quantities of unimportant background information.

Important information, too, might reach the right operator, but have little impact if it was not understood why or how the information was important. The impact of knowing that an air conditioning unit is going down, which cools a room full of GSP (Ground Special Power) equipment, may not be immediately apparent to the LH2 operator. The information may be extremely important for the GSP operator demanding full attention, while only an indication of a remote potential fault in the LH2 system should a series of backup and mitigation processes also fail.

The seemingly bipartite nature (really simple or really complex) of problems experienced suggests that FDIR tools could have an impact by providing:

- External validation of the diagnosis of simple problems

- More information in a broader context of fault propagation possibilities, filtered by relationship to an anomaly

IV. Recommendations

- Additional study of what information is available through console display and other means and how it is presented to the console operators during operations would be useful in a benefit analysis of FDIR tools with respect to what information those tools provide and how that information is presented. A metric of sorts might be developed for the potential impact of FDIR tools on the selection of important information over a quantity of available information.

- Extending the Legacy Benchmarking Task to the EELV GSE systems will both provide data for a system that is closer to the CxP configuration than is the Space Shuttle and provide a basis of comparison and analysis of the current Shuttle system.

- As the development of the FDIR tools proceeds, we would recommend that the end user community be involved as much as possible so as to assure that the final versions of the tools are maximally useful and as free of risk as possible.

- Testing the FDIR tools in as close to an operational environment as possible will facilitate the effective development of the tools.

- Further work is clearly required to make the PRACA database system more consistent and useful to the CxP community. Standards of definition of input quantities as well as a clearer and more consistent process of utilization. These developments could enable the PRACA database to be more useful as a measurement tool for FDIR events, as well as providing insight as to system performance.

Appendix A – PRACA Criticality and Significance Definitions

Critical Item List Criteria.

The following classification of failure modes is included in the CIL:

- All Functional Criticality 1 and 2 items (a single point of failure)
- All Functionality 1R items, where first failure could result in loss of mission, or next failure of any redundant item could cause loss of crew/vehicle
- All Functional Criticality Category 1R and 2R items that fail one or more redundancy screens
- An item which becomes Criticality 1 during intact abort, except for the system causing the abort

Critical Items

Criticality	Criteria
1/1	All
1R/2	All
1R/3	Fails one or more redundancy screens
2/2	All
2R/3	Fails one or more redundancy screens
N/A	Fails to meet Intact Abort requirements.

Criticality

Functional Criticality - Categorization of the effect of loss of all redundancy (like and/or unlike, operational and/or standby) for a given function.

– Functional criticality for redundant items is based upon multiple failures which must occur to result in loss of the system or component function.
– Any hardware item in the failure scenario contributing to or resulting in the effect shall be considered as “redundancy” (like and/or unlike, operational and/or standby).

Functional Criticality	Potential Effect or Failure:
1	Single failure which could result in loss of life or vehicle
1R	Redundant hardware item(s), all of which failed, could cause loss of life or vehicle
2	Single failure which could result in loss of mission
2R	Redundant hardware item(s), all of which failed, could cause loss of mission
3	No effect on mission, crew, or vehicle

Hardware Criticality - Categorization of the worst-case singular direct effect of the identified failure mode of a hardware item.

Hardware Criticality	Potential Effect or Failure
1	Loss of life or vehicle
2	Loss of mission or next failure of any redundant item could cause loss of life or vehicle
3	No effect on mission, crew, or vehicle

Functional and Hardware Criticalities Combinations

Functional Criticality	Hardware Criticality	Potential Effect or Failure
1	1	1/1 - Single failure which could result in loss of life or vehicle.
1R	2	1R/2 - Redundant hardware item(s), all of which failed, could cause loss of life or vehicle. First failure would result in loss of mission or the next failure could cause loss of life or vehicle.
1R	3	1R/3 - Redundant hardware item(s), all of which failed, could cause loss of life or vehicle. First failure has no effect on mission, crew, or vehicle; second failure may result in loss of mission.
2	2	2/2 - Single failure which could result in loss of mission.
2R	3	2R/3 - Redundant hardware item(s), all of which failed, could cause loss of mission. First failure has no effect.
3	3	3/3 - No effect on mission, crew, or vehicle.

These are the only valid combinations of Functional/Hardware Criticalities.
Hardware criticality does not equate to fault tolerance.

Significance

The problems are assigned a Significance Category commensurate with the level of risk or impact the problem or related conditions introduce to the Program/Project.

Significance Category-1 Problems

If the Problem meets or could have resulted in any of the following criteria, it shall be designated as a SC-1 problem.

a. In death of crew and/or loss of vehicle
b. Failure to achieve any major mission objectives/Incremental objectives
c. Involved Failure Modes and Effects Analysis and Critical Items List (FMEA/CIL) Failure Mode with Criticality Classifications 1, 1R, 1S
d. Interruption of schedule, equipment damage, cost overruns
e. Could have resulted in death or major injury/illness

f. Could result in severe, acute, long term or permanent damage to the local ecology, or contribute to regional problems
g. Problem is deemed a "constraint to flight"
h. Early termination of a mission

Significance Category-2 Problems

If the Problem meets or could have resulted in any of the following criteria, it shall be designated as a SC-2 problem.

a. Involved FMEA/CIL Failure Mode with Criticality Classifications 2, 2R
b. Interruption of schedule, equipment damage, or cost overruns at a threshold established by the Project or by the responsible center for the end item or for the activity in work during problem reporting
c. Could have resulted in minor injuries (not covered by basic first aid) or illness
d. Could result in significant impacts to the local ecology, that are recoverable, but would require substantial remedial actions

Significance Category-3 Problems

Problems required to be reported, but not meeting SC-1 or SC-2. Criteria will be categorized SC-3.

Significance Category-4 Problems

Problems not required to be entered into the CxP PRACA information system may be entered as Significance Category-4 problems. SC-4 problems shall be processed in accordance with Project defined requirements.

Due to changes in NSTS 08126, the term "Hardware Criticality" was changed to "part criticality", and "Problem Failure Mode" was changed to "Functional Criticality". Hardware Criticality is described as: "Highest level criticality of the affected part … ." Functional Criticality description changed to add more detail. Described as: "Categorization of the effect of loss of redundancy for a given component or function in the discrepant condition." Or, better stated, the failure mode in the as-found condition.

Appendix B – Problem Processing Requirements for PRACA Data

Requirements for problem processing include the following:

- Uniform criteria for reporting, investigating and analyzing problems.

- Criteria to categorize (or assign) problem significance level to determine the appropriate rigor of technical analysis and management visibility.

- Establish a common work-flow process for closed-loop problem processing, analysis and closure.

- Consolidation of problem history in one central information system (the actual PRACA database) using standardized problem report data elements, coding and terminology

- Identification, implementation and documentation of corrective/preventative action commensurate with the problem significance and risk of recurrence

- Capability to provide problem history across the applicable life cycle of the hardware and software, operations and missions to support trending, evaluate effectiveness of test programs, and the identification of precursors to more serious problems

- Information exchange and providing routine and tailored reports to support problem analysis and support Cx (Constellation) Program/Project organizations such as Safety, Reliability and Quality Assurance (SR&QA), Test and Verification (T&V), Systems Engineering and Integration (SE&I), Configuration Management (CM), Logistics, Ground and Mission Operations, Flight Crew Operations, Crew Exploration Vehicle (CEV)/Crew Launch Vehicle (CLV) maintenance and support, etc.